

# Negacyclic codes over $\mathbb{Z}_4 + u\mathbb{Z}_4$

Rama Krishna Bandi<sup>a,\*</sup>, Maheshanand Bhaintwal<sup>a</sup>

<sup>a</sup> *Department of Mathematics, Indian Institute of Technology Roorkee, Roorkee-247667, INDIA*

---

## Abstract

In this paper, we study negacyclic codes of odd length and of length  $2^k$  over the ring  $R = \mathbb{Z}_4 + u\mathbb{Z}_4$ ,  $u^2 = 0$ . We give the complete structure of negacyclic codes for both the cases. We have obtained a minimal spanning set for negacyclic codes of odd lengths over  $R$ . A necessary and sufficient condition for negacyclic codes of odd lengths to be free is presented. We have determined the cardinality of negacyclic codes in each case. We have obtained the structure of the duals of negacyclic codes of length  $2^k$  over  $R$  and also characterized self-dual negacyclic codes of length  $2^k$  over  $R$ .

**Keywords:** Codes over  $\mathbb{Z}_4 + u\mathbb{Z}_4$ , negacyclic codes, cyclic codes, repeated root cyclic codes.

**2000 MSC:** 94B05, 94B60

---

## 1. Introduction

Cyclic codes are widely studied algebraic codes among all families of codes. Their structure is well known over finite fields [17]. Recently codes over rings have generated a lot of interest after a breakthrough paper by Hammons et al. [15]. When we consider codes over a local ring, a cyclic code is called a distinct roots cyclic code if the code length is relatively prime to the characteristic of the residue field. Their structure over finite chain rings is now well known [19]. They have also been studied over other rings such as  $\mathbb{F}_2 + u\mathbb{F}_2$ ,  $u^2 = 0$ , [7];  $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ ,  $u^2 = v^2 = 0, uv = vu$ , [23];  $\mathbb{F}_2 + v\mathbb{F}_2$ ,  $v^2 = v$ , [25]; and  $\mathbb{Z}_4 + u\mathbb{Z}_4$ ,  $u^2 = 0$  [24, 3]. Via the Gray map, these new families of rings also lead to binary codes with large automorphism groups and in some cases new binary codes.

When the characteristic of the residue field is not relatively prime to the code length then the corresponding cyclic codes is called a repeated root cyclic code. Castangoli [8] et. al. have studied these cyclic codes over finite fields. Lint [16], Tang et. al. [21] and Zimmermann [26] have also explored these codes in their studies. Recently cyclic codes of length  $2^e$  over  $\mathbb{Z}_4$  have been considered by Abualrab and Oehmke in [1, 2]. Blackford [6] has classified cyclic codes of oddly even length (length  $2n$ ,  $n$  is odd) over  $\mathbb{Z}_4$  using Discrete Fourier Transform. Dougherty and Ling [14] have generalized cyclic codes of oddly even length to any even length using the same approach.

Negacyclic codes were first introduced by Berkelamp [4]. They have been generalized to  $\mathbb{Z}_4$  with code length an odd integer by Wolfmann [22]. Blackford [5] has extended the results of [22] to negacyclic codes of even length, and determined all binary linear repeated root cyclic codes that are Gray images of quaternary codes. Dinh and Lopez-Permouth [13] have studied negacyclic codes of odd length in the more general setting of finite chain rings, and also considered repeated root cyclic codes of length  $2^s$  over  $\mathbb{Z}_{2^m}$ . The structure of negacyclic codes of length  $2^s$  over Galois rings and their complete Hamming distances were discussed by Dinh in [12, 9]. Constacyclic codes of length  $2^s$  and  $p^s$  over Galois extension of  $\mathbb{F}_2 + u\mathbb{F}_2$ ,  $u^2 = 0$  and  $\mathbb{F}_{p^s} + u\mathbb{F}_{p^s}$ ,  $u^2 = 0$ , respectively, have been studied by Dinh in [10, 11].

---

\*Corresponding author

Email address: bandi.ramakrishna@gmail.com (Rama Krishna Bandi)

Recently, Yildiz and Karadeniz [24] have studied linear codes over  $R$ . The authors [3] have studied cyclic codes of odd length and length  $2^k$  over  $R$ . The ring  $\frac{R[x]}{\langle x^{2^k}-1 \rangle}$  is a local ring with the unique maximal ideal  $M$  with 3-generators  $2, u, x-1$  (i.e.  $M = \langle 2, u, x-1 \rangle$ ) [3]. The presence of 3 generators makes the characterization of cyclic codes of length  $2^k$  over  $R$  complicated, as was observed in [3]. However, the ring  $\frac{R[x]}{\langle x^{2^k}+1 \rangle}$ , which is also a local ring, has the unique maximal ideal with 2 generators only (See Theorem 17). This motivated us to study negacyclic codes of length  $2^k$  over  $R$ .

The paper is organized as follows: In Section II, we present the preliminaries such as the ring structure of  $R$ , Hensel's lemma, Gray map on  $R$ , etc. We discuss the Galois extension of  $R$  and its ideal structure. In Section III, we have presented a structure of negacyclic codes of odd length over  $R$ , and determined their minimal spanning sets and ranks. We have obtained a necessary and sufficient condition for negacyclic codes of odd length over  $R$  to be free. In Section IV, we have obtained the complete ideal structure of  $\frac{R[x]}{\langle x^{2^k}+1 \rangle}$ . We have classified negacyclic codes of length  $2^k$  and their duals over  $R$ . We have determined the size of each negacyclic code. We have also given the structure of self-orthogonal and self-dual negacyclic codes of length  $2^k$  over  $R$ .

## 2. Preliminaries

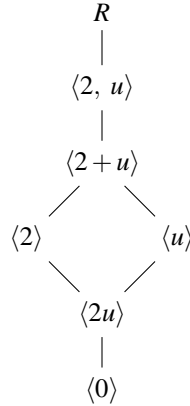
Throughout the paper,  $R$  denotes the ring  $\mathbb{Z}_4 + u\mathbb{Z}_4 = \{a + ub \mid a, b \in \mathbb{Z}_4\}$  with  $u^2 = 0$ .  $R$  can be viewed as the quotient ring  $\mathbb{Z}_4[u]/\langle u^2 \rangle$ . The units of  $R$  are

$$1, 3, 1+u, 1+2u, 1+3u, 3+u, 3+2u, 3+3u,$$

and the non-units are

$$0, 2, u, 2u, 2+u, 2+2u, 3u, 2+3u.$$

$R$  has six ideals in all, and the lattice diagram of these ideals is as follows:



$R$  is a non-principal local ring of characteristic 4 with  $\langle 2, u \rangle$  as its unique maximal ideal.

The image of an element  $f(x) \in R[x]$  in  $\bar{R}[x]$  under the projection map  $R[x] \rightarrow \bar{R}[x]$  is denoted by  $\bar{f}(x)$ . A polynomial  $f(x) \in R[x]$  is called *basic irreducible* (*basic primitive*) if  $\bar{f}(x)$  is an irreducible (primitive) polynomial in  $\bar{R}[x]$ .

A linear code  $C$  of length  $n$  over  $R$  is an  $R$ -submodule of  $R^n$ .  $C$  may not be an  $R$ -free module. A linear code  $C$  of length  $n$  over  $R$  can be expressed as  $C = C_1 + uC_2$ , where  $C_1, C_2$  are linear codes of length  $n$  over  $\mathbb{Z}_4$  as  $R^n = \mathbb{Z}_4^n + u\mathbb{Z}_4^n$ . The Euclidean inner product of any two elements  $x = (x_1, x_2, \dots, x_n)$  and  $y = (y_1, y_2, \dots, y_n)$  of  $R^n$  is defined as  $x \cdot y = x_1y_1 + x_2y_2 + \dots + x_ny_n$ , where the operation is performed

in  $R$ . The dual of a linear code  $C$  is defined as  $C^\perp = \{y \in R^n \mid x \cdot y = 0 \ \forall x \in C\}$ . It follows immediately that if  $C = C_1 + uC_2$  is a linear code over  $R$ , then  $C^\perp = C_1^\perp + uC_2^\perp$ . We define the *rank* of a code  $C$  as the minimum number of generators for  $C$  and the *free rank* of  $C$  as the rank of  $C$  if  $C$  is a free module over  $R$ . There are two other codes associated with  $C$ , namely  $\text{Tor}(C)$  and  $\text{Res}(C)$  and are defined as  $\text{Tor}(C) = \{b \in \mathbb{Z}_4^n : ub \in C\}$  and  $\text{Res}(C) = \{a \in \mathbb{Z}_4^n : a + ub \in C \text{ for some } b \in \mathbb{Z}_4^n\}$ .

A polynomial  $f(x)$  over  $R$  is called a *regular polynomial* if it is not a zero divisor in  $R[x]$ , equivalently,  $f(x)$  is regular if  $\bar{f}(x) \neq 0$ . Two polynomials  $f(x), g(x) \in R[x]$  are said to be *coprime* if there exist  $a(x), b(x) \in R[x]$  such that  $a(x)f(x) + b(x)g(x) = 1$ , or equivalently  $\langle f(x) \rangle + \langle g(x) \rangle = R[x]$ . The following result is well known and has been proved in the present setting in [3].

**Lemma 1.** [3, Lemma 3.4] *Let  $f(x), g(x) \in R[x]$ . Then  $f(x), g(x)$  are coprime if and only if their images  $\bar{f}(x), \bar{g}(x)$  are coprime in  $\bar{R}[x]$ .*

Hensels Lemma [18, Theorem XIII.4] is an important tool in studying local rings, which can lift the factorization into a product of pairwise coprime polynomials over  $\bar{R}$  to such a factorization over  $R$ .

**Theorem 2 (Hensel's Lemma [20]).** *Let  $f$  be a monic polynomial in  $R[x]$  and assume that  $\bar{f} = g_1 g_2 \cdots g_r$ , where  $g_1, g_2, \dots, g_r$  are pairwise coprime monic polynomials over  $\bar{R}$ . Then there exist pairwise coprime monic polynomials  $f_1, f_2, \dots, f_r$  over  $R$  such that  $f = f_1 f_2 \cdots f_r$  in  $R$  and  $\bar{f}_i = g_i, i = 1, 2, \dots, r$ .*

**Theorem 3.** [3, Theorem 3.1] *Let  $g(x) \in \mathbb{F}_2[x]$  be a monic irreducible (primitive) divisor of  $x^{2^r} - 1$ . Then there exists a unique monic basic irreducible (primitive) polynomial  $f(x)$  in  $R[x]$  such that  $\bar{f}(x) = g(x)$  and  $f(x) \mid (x^{2^r-1} - 1)$  in  $R[x]$ .*

We call the polynomial  $f(x)$  in Theorem 3 the *Hensel lift* of  $g(x)$  to  $R$ .

Let  $n$  be an odd integer. Then it follows from [18, Theorem XIII.11] that  $x^n + 1$  factorizes uniquely into pairwise coprime basic irreducible polynomials over  $R$ . Let

$$x^n + 1 = f_1 f_2 \cdots f_m$$

be such a factorization of  $x^n + 1$ . Then it follows from the Chinese Remainder Theorem that

$$\frac{R[x]}{\langle x^n + 1 \rangle} = \oplus_{i=1}^m \frac{R[x]}{\langle f_i \rangle}.$$

Therefore every ideal  $I$  of  $\frac{R[x]}{\langle x^n + 1 \rangle}$  can be expressed as  $I = \oplus_{i=1}^m I_i$ , where  $I_i$  is an ideal of the ring  $\frac{R[x]}{\langle f_i \rangle}$ ,  $i = 1, 2, \dots, m$ .

Now we consider the Galois extension of  $R$ . Let  $f(x)$  be a basic irreducible polynomial of degree  $r$  in  $R[x]$ . Then the Galois extension of  $R$  is defined as the quotient ring  $\frac{R[x]}{\langle f(x) \rangle}$  and is denoted by  $GR(R, r)$ .

The authors have discussed in [3] the Galois extension of  $R$  and proved that the ring  $GR(R, r)$  is a local ring with unique maximal ideal  $\langle \langle 2, u \rangle + \langle f \rangle \rangle$  and the residue field  $\mathbb{F}_{2^r}$ .

Let  $\mathcal{T} = \{0, 1, \xi, \xi^2, \dots, \xi^{2^r-2}\}$  be the *Teichmüller* representatives of  $GR(R, r)$ , where  $\xi$  is a root of a basic primitive polynomial of degree  $r$  in  $R[x]$ . An element  $x$  of  $GR(R, r)$  can be represented as  $x = a_0 + 2a_1 + ua_2 + 2ua_3$ , where  $a_0, a_1, a_2, a_3 \in \mathcal{T}$ . A non-zero element  $x = a_0 + 2a_1 + ua_2 + 2ua_3$  of  $GR(R, r)$  is unit if and only if  $a_0$  is non-zero in  $\mathcal{T}$  [3].

Thus the group of units of  $GR(R, r)$  [3], denoted by  $GR(R, r)^*$ , is given by

$$GR(R, r)^* = \{a_0 + 2a_1 + ua_2 + 2ua_3 : a_0, a_1, a_2, a_3 \in \mathcal{T}, a_0 \neq 0\}.$$

The set of all zero divisors of  $GR(R, r)$  is given by  $\{2a_1 + ua_2 + 2ua_3 : a_1, a_2, a_3 \in \mathcal{T}\}$ , which is the maximal ideal generated by  $\langle 2, u \rangle$  in  $GR(R, r)$ .

The following theorem gives the ideal structure of  $GR(R, r) = \frac{R[x]}{\langle f \rangle}$ .

**Theorem 4.** [3, Theorem 3.5] *Let  $f \in R[x]$  be a basic irreducible polynomial. Then the ideals of  $\frac{R[x]}{\langle f \rangle}$  are precisely,  $\{0\}, \langle 1 + \langle f \rangle \rangle, \langle 2 + \langle f \rangle \rangle, \langle u + \langle f \rangle \rangle, \langle 2u + \langle f \rangle \rangle, \langle 2 + u + \langle f \rangle \rangle$  and  $\langle \langle 2, u \rangle + \langle f \rangle \rangle$ .*

### 3. Negacyclic codes of odd lengths over $\mathbb{Z}_4 + u\mathbb{Z}_4$

Let  $\lambda$  be a unit in  $R$ . A linear code  $C$  of length  $n$  over  $R$  is said to be  $\lambda$ -constacyclic code if  $C$  is invariant under  $\lambda$  cyclic shifts, i. e., if  $(c_0, c_1, \dots, c_{n-1}) \in C$ , then  $(\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$ . If  $\lambda = -1$ , then  $C$  is called a *negacyclic code*. For  $\lambda = 1$  negacyclic codes coincide with cyclic codes.

In the polynomial representation of elements of  $R_n$ , a  $\lambda$ -constacyclic code of length  $n$  over  $R$  is an ideal of  $\frac{R[x]}{\langle x^n - \lambda \rangle}$ . In particular for  $\lambda = -1$ , a negacyclic code is an ideal of  $\frac{R[x]}{\langle x^n + 1 \rangle}$ .

Let  $g(x) = g_0 + g_1x + g_2x^2 + \dots + g_rx^r$  be a polynomial in  $R_n$ . Then the reciprocal of  $g(x)$  is the polynomial  $g^*(x) = x^r g(\frac{1}{x}) = g_r + g_{r-1}x + g_{r-2}x^2 + \dots + g_0x^r$  in  $R_n$ . If  $I$  is an ideal of  $R_n$ , then so is  $A(I)^*$ , where  $A(I)^* = \{g^*(x) : g(x) \in A(I)\}$ . It is well known that if  $C$  is a negacyclic code, then  $C^\perp = A(C)^*$ .

**Theorem 5.** *If  $C = C_1 + uC_2$  is a  $\lambda$ -constacyclic code of length  $n$  over  $R$ , then  $C_1$  is either a cyclic code or a negacyclic code of length  $n$  over  $\mathbb{Z}_4$ .*

PROOF. Let  $T_\lambda$  be the  $\lambda$ -constacyclic shift operator on  $R^n$ . Let  $C$  be a  $\lambda$ -constacyclic code of length  $n$  over  $R$ . Let  $(a_0, a_1, \dots, a_{n-1}) \in C_1$ ,  $(b_0, b_1, \dots, b_{n-1}) \in C_2$ . Then the corresponding element of  $C$  is  $c = (c_0, c_1, \dots, c_{n-1}) = (a_0, a_1, \dots, a_{n-1}) + u(b_0, b_1, \dots, b_{n-1}) = (a_0 + ub_0, a_1 + ub_1, \dots, a_{n-1} + ub_{n-1})$ . Since  $C$  is a  $\lambda$ -constacyclic code, so  $T_\lambda(c) = (\lambda c_{n-1}, c_0, c_1, \dots, c_{n-2}) \in C$ , where  $c_i = a_i + ub_i$ . Let  $\lambda = \alpha + u\beta$ , where  $\alpha, \beta \in \mathbb{Z}_4$ . Then  $T_\lambda(c) = (\alpha a_{n-1}, a_0, \dots, a_{n-2}) + u((\alpha b_{n-1} + \beta a_{n-1}), b_0, \dots, b_{n-2})$ . Since the units of  $\mathbb{Z}_4$  are 1 and  $-1$ , so  $\alpha = \pm 1$ . Hence the result.  $\square$

**Corollary 6.** *If  $C$  is a negacyclic code of length  $n$  over  $R$ , then both  $C_1$  and  $C_2$  are negacyclic codes over  $\mathbb{Z}_4$ .*

PROOF. Since  $\lambda = -1$ , so  $\alpha = -1, \beta = 0$ . Then we get  $T_\lambda(c) = (-a_{n-1}, a_0, \dots, a_{n-2}) + u(-b_{n-1}, b_0, \dots, b_{n-2})$  for some  $c \in C$ , from which follows that  $C_1, C_2$  are negacyclic.  $\square$

For the rest of this section, we assume that  $n$  is odd. Define  $\phi : \frac{R[x]}{\langle x^n - 1 \rangle} \rightarrow \frac{R[x]}{\langle x^n + 1 \rangle}$  such that  $\phi(f(x)) = f(-x)$ . It was shown in [13, Theorem 5.1] that the map  $\phi$  is a ring isomorphism when  $R$  is a finite chain ring. The result can easily be extended to arbitrary finite local rings. Therefore  $I$  is an ideal of  $\frac{R[x]}{\langle x^n - 1 \rangle}$  if and only if  $J = \phi(I)$  is an ideal of  $\frac{R[x]}{\langle x^n + 1 \rangle}$ .

**Theorem 7.**  *$C$  is a cyclic code of length  $n$  over  $R$  if and only if  $\phi(C)$  is a negacyclic code over  $R$ .*

PROOF. Let  $\tau$  and  $\tau'$  be cyclic and negacyclic shifts. Then the result follows from the fact that  $\phi \circ \tau = \tau' \circ \phi$ .  $\square$

The following results (Theorem 8 through Theorem 14) are discussed for cyclic codes over  $R$  in [3], and are straightforward generalizations thereof via the isomorphism  $\phi$  defined above. So we present them here without proofs.

**Theorem 8.** [3, Theorem 4.1] *The ring  $R_n = \frac{R[x]}{\langle x^n + 1 \rangle}$  is not a principal ideal ring.*

Therefore, a negacyclic code of length  $n$  over  $R$  is in general not principally generated. Since  $n$  is odd, the ring  $\frac{\mathbb{Z}_4[x]}{\langle x^n + 1 \rangle}$  is a principal ideal ring. Therefore a negacyclic code of length  $n$  over  $R$  is of the form  $C = C_1 + uC_2 = \langle g_1 \rangle + u \langle g_2 \rangle$ , where  $g_1, g_2 \in \mathbb{Z}_4[x]$  are generator polynomials of the negacyclic codes  $C_1, C_2$ , respectively.

It follows from the Chinese Remainder Theorem that a negacyclic code of length  $n$  over  $R$  is sum of the ideals listed in Theorem 4.

**Theorem 9.** [3, Corollary 1] *The number of negacyclic codes of length  $n$  over  $R$  is  $7^m$ , where  $m$  is the number of distinct basic irreducible factors of  $x^n + 1$ .*

The following result gives a sufficient condition for a negacyclic code  $C$  over  $R$  to be a free  $\mathbb{Z}_4$ -code.

**Theorem 10.** [3, Theorem 4.4] *Let  $C = C_1 + uC_2$  be a negacyclic code of length  $n$  over  $R$ . If  $C_1, C_2$  are free codes over  $\mathbb{Z}_4$ , then  $C$  is a free  $\mathbb{Z}_4$ -module.*

The converse of the above theorem is in general not true, i.e., if a negacyclic code  $C = C_1 + uC_2$  is a free  $\mathbb{Z}_4$ -module of length  $n$  over  $R$ , then  $C_1$  or  $C_2$  may not be a free code of length  $n$  over  $\mathbb{Z}_4$  (see Example 2). However, if  $C$  is an  $R$ -free module (code) of length  $n$  over  $R$ , then  $C_1$  must be a free code over  $\mathbb{Z}_4$  (see Theorem 14).

**Example 1.** The polynomial  $x^{15} - 1$  factorizes into irreducible polynomials over  $\mathbb{F}_2$  as  $x^{15} - 1 = (x - 1)(x^4 + x^3 + 1)(x^4 + x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)$ . The Hensel lifts of  $x^4 + x^3 + 1, x^4 + x + 1, x^4 + x^3 + x^2 + x + 1$  and  $x^2 + x + 1$  to  $\mathbb{Z}_4$  are  $x^4 - x^3 + 2x^2 + 1, x^4 + 2x^2 - x + 1, x^4 + x^3 + x^2 + x + 1$  and  $x^2 + x + 1$ , respectively. Therefore  $x^{15} - 1 = (x - 1)(x^4 - x^3 + 2x^2 + 1)(x^4 + 2x^2 - x + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)$ . Replacing  $x$  by  $-x$ , we get  $x^{15} + 1 = (x + 1)(x^4 + x^3 + 2x^2 + 1)(x^4 + 2x^2 + x + 1)(x^4 - x^3 + x^2 - x + 1)(x^2 - x + 1)$ . Define  $C = \langle x^4 - x^3 + x^2 - x + 1 \rangle + u \langle x^4 + 2x^2 + x + 1 \rangle$ . Then  $C$  is a negacyclic code of length 15 over  $R$ , which is also a free  $\mathbb{Z}_4$ -module.

**Example 2.** Let  $C = C_1 + uC_2$  be a free  $\mathbb{Z}_4$ -negacyclic code of length 7 over  $R$  generated by  $g(x) = 2x^2 + u(x^3 + x + 1)$ . Then  $C_1$  is a negacyclic code of length 7 over  $\mathbb{Z}_4$  generated by  $g(x) \pmod{u} = g_1(x) = 2x^2$ . Since  $g_1(x)$  is a zero divisor, so  $C_1$  is not  $\mathbb{Z}_4$ -free.

The general form of a cyclic code  $\mathcal{C}$  of length  $n$  over  $R$  is given by  $\mathcal{C} = \langle g(x) + up(x), ua(x) \rangle$ , where  $g(x), p(x), a(x) \in \mathbb{Z}_4[x]$  [3]. The same structure can be adopted to the negacyclic codes of length  $n$  over  $R$  through the isomorphism  $\phi$  defined earlier in this section. Thus a negacyclic code  $C$  of length  $n$  over  $R$  can be expressed as  $\mathcal{C} = \langle g(x) + up(x), ua(x) \rangle$ , where  $g(x), p(x), a(x) \in \mathbb{Z}_4[x]$ .

Theorem 11 and Theorem 12 below give the minimal spanning set of negacyclic code over  $R$ .

**Theorem 11.** [3, Theorem 4.8] *Let  $C$  be a negacyclic code of length  $n$  over  $R$ . If  $C = \langle g(x) + up(x), ua(x) \rangle$ ,  $\deg g(x) = k_1$  and  $\deg a(x) = k_2$ , then  $C$  has rank  $2n - k_1 - k_2$  and a minimal spanning set  $A = \{(g(x) + up(x)), x(g(x) + up(x)), x^2(g(x) + up(x)), \dots, x^{n-k_1-1}(g(x) + up(x)), ua(x), xua(x), x^2ua(x), \dots, x^{n-k_2-1}ua(x)\}$ .*

**Theorem 12.** [3, Theorem 4.10] *Let  $C = \langle g(x) + up(x), ua(x) \rangle$  be a negacyclic code of length  $n$  over  $R$ , and  $g(x)$  is regular and  $a(x)$  is monic with  $\deg g(x) = k_1$  and  $\deg a(x) = k_2$ , respectively. Then  $C$  has rank  $n - k_2$  and a minimal spanning set  $B = \{(g(x) + up(x)), x(g(x) + up(x)), x^2(g(x) + up(x)), \dots, x^{n-k_1-1}(g(x) + up(x)), ua(x), xua(x), x^2ua(x), \dots, x^{k_1-k_2-1}ua(x)\}$ .*

**Example 3.** Consider the negacyclic code  $C$  of length 7 over  $R$  generated by the polynomial  $g(x) = x^3 + (2 + u)x^2 + (1 + u)x + (1 + u)$  and  $a(x) = x + 1$ . Then the rank of  $C$  is 6 and a minimal spanning set of  $C$  is  $\{g(x), xg(x), x^2g(x), x^3g(x), ua(x), xua(x)\}$ .

In Theorem 11 and Theorem 12, we have only seen minimal spanning sets of negacyclic codes over  $R$ . However we can find a basis for negacyclic code of length  $n$  when it is principally generated. The following theorem gives a necessary and sufficient condition for the negacyclic codes over  $R$  to be free.

**Theorem 13.** [3, Proposition 1] *Let  $C$  be a principally generated negacyclic code of length  $n$  over  $R$ . Then  $C$  is free if and only if there exists a monic generator  $g(x)$  in  $C$  such that  $g(x) \mid x^n + 1$ . Furthermore,  $C$  has free rank  $n - \deg g(x)$  and the elements  $g(x), xg(x), \dots, x^{n-\deg g(x)-1}g(x)$  form a basis for  $C$ .*

**Example 4.** Consider the negacyclic code  $C$  of length 15 over  $R$  generated by the polynomial  $g(x) = x^4 + 2x^2 + x + 1$ , where  $g(x)$  is the Hensel lift of  $x^4 + x + 1 \in \mathbb{F}_2[x]$  to  $R$  and  $g(x) \mid x^{15} + 1$ . The negacyclic code  $C = \langle g(x) \rangle$  is an  $R$ -free negacyclic code of length 15 and the free rank 11.

**Theorem 14.** [3, Theorem 5.4] *If  $C = C_1 + uC_2$  is a free negacyclic code of length  $n$  over  $R$ , then so is  $C_1$  over  $\mathbb{Z}_4$ .*

**Example 5.** Consider again the negacyclic code  $C$  of length 15 generated by  $g(x) = x^4 + 2x^2 + x + 1$ . Then  $C$  is free over  $R$ , as  $x^4 + 2x^2 + x + 1$  is a divisor of  $x^{15} + 1$  over  $R$ . Since  $x^4 + 2x^2 + x + 1$  is a divisor of  $x^{15} + 1$  over  $\mathbb{Z}_4$  as well, so  $C_1$  is a free negacyclic code of length 15 over  $\mathbb{Z}_4$ .

#### 4. Negacyclic codes of length $2^k$

So far we considered negacyclic codes with the assumption that the code length  $n$  is coprime to the characteristic of the ring  $R$ , i.e.,  $(n, 4) = 1$ . Now we extend our study to negacyclic codes of length  $n = 2^k$ ,  $k \geq 1$ .  $(n, 4) \neq 1$ . Negacyclic codes whose lengths are not relatively prime to characteristic of  $R$  are known as repeated root negacyclic codes.

**Lemma 15.** [23] *Every non-zero, non-unit element of  $R_n = \frac{R[x]}{\langle x^n + 1 \rangle}$  must be a zero divisor.*

The following result is a generalization of [3, Theorem 6.2].

**Theorem 16.** *The ring  $R_n$  is not a local ring when  $n = 2^k m$ , where  $m = 4d + 1$  ( $d \geq 1$ ) or  $m = 4d + 3$  ( $d \geq 0$ ).*

**Theorem 17.** *The ring  $R_n$  is a local ring when  $n = 2^k$  where  $k \geq 1$ .*

PROOF. Define the map  $\Phi : R_n \rightarrow \frac{\mathbb{Z}_4[x]}{\langle x^n + 1 \rangle}$  such that  $\Phi(f(x)) = f_1(x) \pmod{u}$ , where  $f(x) = f_1(x) + uf_2(x)$ . It is easy to verify that  $\Phi$  is a surjective ring homomorphism. It is well known that the ring  $\frac{\mathbb{Z}_4[x]}{\langle x^{2^k} + 1 \rangle}$  is a local ring with the unique maximal ideal  $\langle x + 1 \rangle$  [12]. The inverse image of the maximal ideal  $\langle x + 1 \rangle$  is  $\Phi^{-1}(\langle x + 1 \rangle) = \langle u, x + 1 \rangle$ . Since  $\langle u, x + 1 \rangle$  contains all non-units of  $R_n$ , so it is unique maximal ideal of  $R_n$  and hence  $R_n$  is local.  $\square$

Now onward  $n = 2^k$ ,  $k \geq 1$ . Also, now onward, we prefer to express a polynomial in terms of  $x + 1$ , rather than in  $x$ , to make the computations easier in  $R_n$ . Each polynomial in  $R_n$  can uniquely be written as  $\sum_{j=0}^{n-1} f_j(x+1)^j$ ,  $f_j \in R$ , and such a polynomial is denoted by  $f(x)$ .

$$\text{Let } R'_n = \frac{\mathbb{Z}_4[x]}{\langle x^n + 1 \rangle} \text{ and } R''_n = \frac{\mathbb{Z}_2[x]}{\langle x^n + 1 \rangle}.$$

**Lemma 18.** *In  $R_n$ ,  $(x + 1)^n = 2x^{\frac{n}{2}}$  and  $(x + 1)$  is nilpotent with nilpotency  $2n$ .*

PROOF. It can easily be seen by induction that  $(x + 1)^n = x^n + 1 + 2x^{\frac{n}{2}}$  in  $R_n$ . Since  $x^n = -1$  in  $R_n$ , so  $(x + 1)^n = 2x^{\frac{n}{2}}$ . From this follows that  $(x + 1)^{2n} = 0$ . Also there is no  $l < 2n$  such that  $(x + 1)^l = 0$  in  $R_n$ . For if, there any  $n < l < 2n$  such that  $(x + 1)^l = 0$ , then we get  $2(x + 1)^{l-n} = 0$ , since  $(x + 1)^l = (x + 1)^n(x + 1)^{l-n} = 2x^{\frac{n}{2}}(x + 1)^{l-n}$  and  $x^{\frac{n}{2}}$  is a unit in  $R_n$ . But  $2(x + 1)^{l'} \neq 0$  for any  $l' < n$  in  $R_n$ . Hence  $2n$  is the nilpotency of  $x + 1$ .  $\square$

**Lemma 19.** *An element  $f(x) = \sum_{j=0}^{n-1} a_j(x + 1)^j$  is a unit in  $R_n$  if and only if  $a_0$  is a unit in  $R$ .*

**Lemma 20.** In  $R_n$ ,  $(x+1)^n = 2x^{\frac{n}{2}} = 2\left((x+1)^{\frac{n}{2}} + 1\right)$  and also  $\langle (x+1)^n \rangle = \langle 2 \rangle$ .

An element  $f(x)$  in  $R_n$  can be written as  $f(x) = f_1(x) + uf_2(x)$ , where  $f_i(x) \in R'_n$ . An element  $f(x)$  in  $R_n$  is called a *monic element* if  $f(x)$  is a monic polynomial in  $R_n$ . Now we consider the ideal structure of  $R_n$ .

Define  $\psi : R \rightarrow \mathbb{Z}_4$  such that  $\psi(a+bu) = a \pmod{u}$ . It can easily be seen that  $\psi$  is a ring homomorphism with  $\ker \psi = \langle u \rangle = u\mathbb{Z}_4$ . Extend  $\psi$  to the homomorphism  $\Phi : R_n \rightarrow R'_n$  such that  $\Phi(a(x) + ub(x)) = a(x) \pmod{u}$ , where  $a(x), b(x) \in \mathbb{Z}_4[x]$ . Let  $I$  be an ideal of  $R_n$ . Restrict  $\Phi$  to  $I$  and define

$$J = \{h(x) \in R'_n : uh(x) \in \ker \Phi\}.$$

Clearly  $J$  is an ideal of  $R'_n$ . Since  $R'_n$  is finite chain ring with the maximal ideal  $\langle x+1 \rangle$ , so  $J = \langle (x+1)^m \rangle$  for some  $1 \leq m \leq 2n$ . Therefore  $\ker \Phi = \langle u(x+1)^m \rangle$ . Similarly, the image of  $I$  under  $\Phi$  is an ideal of  $R'_n$  and  $\Phi(I) = \langle (x+1)^s \rangle$  for some  $1 \leq s \leq 2n$ . Hence  $I = \langle (x+1)^s + up(x), u(x+1)^m \rangle$  for some  $p(x) = \sum_{j=0}^{n-1} p_j(x+1)^j \in \mathbb{Z}_4[x]$ . Since  $u(x+1)^s = u((x+1)^s + up(x)) \in C$  and  $\Phi(u(x+1)^s) = 0$ , so  $(x+1)^m \mid (x+1)^s$ . This implies that  $m \leq s$ . When  $m = s$ , we get  $u(x+1)^m \in \langle (x+1)^s + up(x) \rangle = I$ . Now let  $m < s$ . Then a non-trivial ideal  $I$  of  $R_n$  has the form

$$I = \left\langle (x+1)^s + u \sum_{j=0}^{n-1} p_j(x+1)^j, u(x+1)^m \right\rangle, \quad 1 \leq s \leq 2n-1 \text{ and } 0 \leq m \leq s-1.$$

When  $m < n$ ,

$$I = \left\langle (x+1)^s + u \sum_{j=0}^{n-1} p_j(x+1)^j, u(x+1)^m \right\rangle = \left\langle (x+1)^s + u \sum_{j=0}^{m-1} p_j(x+1)^j, u(x+1)^m \right\rangle.$$

Therefore

$$I = \left\langle (x+1)^s + u \sum_{j=0}^{\min\{m-1, n-1\}} p_j(x+1)^j, u(x+1)^m \right\rangle.$$

If  $t$  is the smallest non-zero integer such that  $p_t$  is non-zero, then a polynomial  $f(x) = (x+1)^s + u \sum_{j=0}^{n-1} p_j(x+1)^j \in R[x]$  can be represented as  $f(x) = (x+1)^s + u(x+1)^t h(x)$ , where  $h(x) \in \mathbb{Z}_4[x]$  and  $\deg h(x) \leq n-t-1$ . Hence  $I$  can be written as

$$I = \langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle,$$

where  $1 \leq s \leq 2n-1, 0 \leq t < \min\{m, n\}, 0 \leq m \leq s-1$  and  $h(x) \in \mathbb{Z}_4[x]$ .

Summarizing this discussion, we present the complete ideal structure of  $R_n$  in the following theorem.

**Theorem 21.** Let  $I$  be an ideal in  $R_n$ . Then  $I$  is one of the following:

1. *Trivial ideals:*  
 $\langle 0 \rangle$  or  $\langle 1 \rangle$ .
2. *Principal ideals:*
  - (a)  $\langle u(x+1)^m \rangle, 0 \leq m \leq 2n-1$
  - (b)  $\langle (x+1)^s + u(x+1)^t h(x) \rangle, 1 \leq s \leq 2n-1, 0 \leq t < \min\{s, n\}$ .
3. *Non-principal ideals:*  
 $\langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle, 1 \leq s \leq 2n-1, 0 \leq t < \min\{m, n\}, 0 \leq m \leq s-1$ .

The ideals described in Theorem 21 are not distinct. For instance, in  $R_2$ , the ideals  $\langle (x+1)^3 + u \rangle$  and  $\langle (x+1)^3 + u(1 + (x+1)) \rangle$  are same, since  $(x+1)^3 + u(1 + (x+1)) = ((x+1)^3 + u)(1 + (x+1))$ , as  $(1 + (x+1))$  is a unit in  $R_n$ . Similarly, the ideals  $\langle (x+1)^2 + u \rangle$  and  $\langle (x+1)^2 + 3u \rangle$  are also same. But the ideals  $\langle (x+1)^2 + u \rangle$  and  $\langle (x+1)^2 + u(1 + (x+1)) \rangle$  are distinct, as  $u(x+1)$  is neither in  $\langle (x+1)^2 + u \rangle$  nor  $\langle (x+1)^2 + u(1 + (x+1)) \rangle$ . So it is very important to find the smallest value of  $T$  such that  $u(x+1)^T \in \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , through which the repetition of ideals can be avoided and ideals (negacyclic codes) can be determined distinctly.

**Theorem 22.** *Let  $T$  be the smallest non-negative integer such that*

$$u(x+1)^T \in I = \langle (x+1)^s + u(x+1)^t h(x) \rangle,$$

*where  $1 \leq s \leq n-1$ ,  $0 \leq t < s$ ,  $h(x) \in \mathbb{Z}_4[x]$  and  $\deg h(x) \leq s-t-1$ . Then  $T = s$ .*

**Theorem 23.** *Let  $I = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $n \leq s \leq 2n-1$  and  $\deg h(x) \leq n-t-1$ . Then there exists a non-negative integer  $T < n$  such that  $u(x+1)^T \in I$  if and only if  $h(x)$  is a unit in  $R'_n$  and  $t < s-n$ . Moreover, if  $T$  is the smallest of such non-negative integers, then  $T = 2n-s+t$ .*

**Theorem 24.** *Let  $T$  be the smallest non-negative integer such that  $u(x+1)^T \in \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $n \leq s \leq 2n-1$ ,  $t \geq s-n$ ,  $h(x)$  is a unit in  $R'_n$  and  $\deg h(x) \leq n-t-1$ . Then  $T \geq n$  and  $T = \min\{s, 2n-s+t\}$ .*

Theorem 23 and Theorem 24 give the value of  $T$  such that  $u(x+1)^T \in I$ , only when  $h(x)$  is a unit in  $\frac{\mathbb{Z}_4[x]}{(x^n+1)}$ . If  $h(x)$  is not a unit in  $\frac{\mathbb{Z}_4[x]}{(x^n+1)}$ , then we can have either  $h(x) = 2h'(x)$  or  $h(x) = 2h_1(x) + (x+1)^l h_2(x)$ , where  $h'(x)$ ,  $h_1(x)$  and  $h_2(x)$  are units in  $R''_n$ ,  $R'_n$ , respectively. For example,

$$\begin{aligned} h(x) &= 2 + 2(x+1) + (x+1)^3 + 3(x+1)^4 + 2(x+1)^5 + (x+1)^6 + 3(x+1)^7 \\ &= 2(1 + (x+1) + (x+1)^5) + (x+1)^3(1 + 3(x+1) + (x+1)^3 + 3(x+1)^3) \\ &= 2h_1(x) + (x+1)^3 h_2(x), \end{aligned}$$

where  $h_1(x)$ ,  $h_2(x)$  are units in  $R''_n$ ,  $R'_n$ , respectively.

Now we will find the smallest value of  $T$  in these two cases of  $h(x)$  also.

**Theorem 25.** *Let  $T$  be the smallest non-negative integer such that*

$$u(x+1)^T \in \langle (x+1)^s + 2u(x+1)^t h(x) \rangle,$$

*where  $n \leq s \leq 2n-1$ ,  $0 \leq t < n$  and  $h(x)$  is a unit in  $R''_n$ . Then  $t < s-n$  and  $T = \min\{s, 3n-s+t\}$ .*

**Theorem 26.** *Let  $T$  be the smallest non-negative integer such that*

$$u(x+1)^T \in \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)) \rangle,$$

*where  $n \leq s \leq 2n-1$ ,  $0 \leq t < n$ ,  $h_1(x)$  and  $h_2(x)$  are units in  $R''_n$ . Then  $T = \min\{s, 2n-s+t+l\}$ .*

PROOF. The proof is similar to that of Theorem 25. □

We summarize the value of  $T$  for different cases of  $h(x)$ ,  $s$  and  $t$  in the following remarks.



**Remark 1.** In view of Theorems 22 through 26, if  $0 \leq T \leq 2n-1$  is the smallest non-negative integer such that  $u(x+1)^T \in I = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $0 \leq s \leq 2n-1$  and  $\deg h(x) \leq n-t-1$ , then

$$T = \begin{cases} s & \text{if } 1 \leq s \leq n-1, \\ 2n-s+t & \text{if } n \leq s \leq 2n-1, 0 \leq t < 2s-2n \text{ and } h(x) \text{ is a unit in } R'_n, \\ s & \text{if } n \leq s \leq 2n-1 \text{ and } t \geq 2s-2n, \text{ and } h(x) \text{ is a unit in } R'_n, \\ 3n-s+t & \text{if } n < s \leq 2n-1, 0 \leq t < 2s-3n \text{ and } h(x) = 2h'(x), \\ s & \text{if } n < s \leq 2n-1, 2s-3n \leq t < s-n \text{ and } h(x) = 2h'(x), \\ 2n-s+l+t & \text{if } n < s \leq 2n-1, 0 \leq t < 2s-2n, 0 \leq l+t < 2s-2n \text{ and } h(x) = 2h_1(x) + (x+1)^l h_2(x), \\ s & \text{if } n < s \leq 2n-1, 0 \leq t < s-n, l+t \geq 2s-2n \text{ and } h(x) = 2h_1(x) + (x+1)^l h_2(x). \end{cases}$$

**Remark 2.** If  $0 \leq T_1 \leq n-1$  is the smallest non-negative integer such that  $2u(x+1)^{T_1} \in I = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $0 \leq s \leq 2n-1$  and  $\deg h(x) \leq n-t-1$ , then

$$T_1 = \begin{cases} 0 & \text{if } 1 \leq s \leq n-1, \\ 0 & \text{if } n \leq s \leq 2n-1, 0 \leq t < s-n \text{ and } h(x) \text{ is a unit in } R'_n, \\ n-s+t & \text{if } n \leq s \leq 2n-1, s-n \leq t < 2s-2n \text{ and } h(x) \text{ is a unit in } R'_n, \\ s-n & \text{if } n \leq s \leq 2n-1, 2s-2n \leq t < n \text{ and } h(x) \text{ is a unit in } R'_n, \\ 2n-s+t & \text{if } n < s \leq 2n-1, 0 \leq t < 2s-3n \text{ and } h(x) = 2h'(x), \\ s-n & \text{if } n < s \leq 2n-1, 2s-3n \leq t < s-n \text{ and } h(x) = 2h'(x), \\ 0 & \text{if } n \leq s \leq 2n-1, 0 \leq t < s-n, 0 \leq l+t \leq s-n \text{ and } h(x) = 2h_1(x) + (x+1)^l h_2(x), \\ l+t-s+n & \text{if } n < s \leq 2n-1, 0 \leq t < s-n, s-n < l+t < 2s-2n \text{ and } h(x) = 2h_1(x) + (x+1)^l h_2(x), \\ s-n & \text{if } n < s \leq 2n-1, 0 \leq t < s-n, l+t \geq 2s-2n \text{ and } h(x) = 2h_1(x) + (x+1)^l h_2(x). \end{cases}$$

Now we can distinguish the ideals of  $R_n$ . The following theorem gives the distinct monic principal ideals of  $R_n$ .

**Theorem 27.** The distinct monic principal ideals of  $R_n$  are

1.  $I = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $1 \leq s \leq n-1, 0 \leq t < s$ ,  $h(x)$  is either zero or a unit in  $R''_n$  and  $\deg h(x) \leq s-t-1$ .
2.  $I = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $n \leq s \leq 2n-1, 0 \leq t < n$ ,  $h(x)$  is either zero or a unit in  $R''_n$  and  $\deg h(x) \leq T-t-1 = \begin{cases} 2n-s-1 & \text{if } t < s-n, \\ n-t-1 & \text{if } t \geq s-n. \end{cases}$
3.  $I = \langle (x+1)^s + 2u(x+1)^t h(x) \rangle$ , where  $n < s \leq 2n-1, 0 \leq t < s-n$ ,  $h(x)$  is a unit in  $R''_n$  and  $\deg h(x) \leq T_1-t-1 = \begin{cases} 2n-s-1 & \text{if } t < 2s-3n, \\ s-n-t-1 & \text{if } t \geq 2s-3n. \end{cases}$
4.  $I = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)) \rangle$ , where  $n < s \leq 2n-1, 0 \leq t < s-n, l > s-n-t$ ,  $h_1(x), h_2(x)$  are units in  $R''_n$ ,  $\deg h_1(x) \leq T_1-t-1$  and  $\deg h_2(x) \leq n-t-l-1$ .

Using the above principal ideals of  $R_n$ , the non-principal ideals can be described as follows:

**Theorem 28.** The distinct non-principal ideals of  $R_n$  are

1.  $I = \langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $1 \leq s \leq n-1, 0 \leq t < m < s$ ,  $h(x)$  is either zero or a unit in  $R''_n$  and  $\deg h(x) \leq m-t-1$ .
2.  $I = \langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n \leq s \leq 2n-1, 0 \leq t < n, 1+t \leq m < T$ ,  $h(x)$  is either zero or a unit in  $R''_n$  and  $\deg h(x) \leq \min\{m, n\} - t - 1$ .

3.  $I = \langle (x+1)^s + 2u(x+1)^t h(x), u(x+1)^m \rangle$ ,  
where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m < T$ ,  $h(x)$  is a unit in  $R_n''$  and  $\deg h(x) \leq \min\{m, T_1\} - t - 1$ .
4.  $\langle (x+1)^s + 2u(x+1)^t h(x), 2u(x+1)^{m_1} \rangle$ ,  
where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m_1 < T_1$ ,  $h(x)$  is a unit in  $R_n''$  and  $\deg h(x) \leq m_1 - t - 1$ .
5.  $I = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), u(x+1)^m \rangle$ ,  
where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $t+l < m < n$ ,  $h_1(x), h_2(x)$  are units in  $R_n''$ ,  $\deg h_1(x) < T_1$ ,  $\deg h_2(x) < n-t-l$ .
6.  $\langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), 2u(x+1)^m_1 \rangle$ ,  
where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $\deg h_1(x) < m_1 < \min\{s-n, n-s+l+t\}$ ,  $h_1(x), h_2(x)$  are units in  $R_n''$ .

**Theorem 29.** Let  $C$  be a negacyclic code of length  $n$  over  $R$ . Then  $C$  is one of the following:

- **Type 0:**  $\langle 0 \rangle$  or  $\langle 1 \rangle$ .
- **Type 1:**  $\langle u(x+1)^m \rangle$ ,  $0 \leq m \leq 2n-1$ .
- **Type 2.0:**  $\langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $1 \leq s \leq n-1$ ,  $0 \leq t < s$ ,  $h(x)$  is either zero or a unit in  $R_n''$  and  $\deg h(x) \leq s-t-1$ .
- **Type 2.1:**  $\langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $n \leq s \leq 2n-1$ ,  $0 \leq t < n$ ,  
 $h(x)$  is either zero or a unit in  $R_n''$  and  $\deg h(x) \leq T-t-1 = \begin{cases} 2n-s-1 & \text{if } t < s-n, \\ n-t-1 & \text{if } t \geq s-n. \end{cases}$
- **Type 2.2:**  $\langle (x+1)^s + 2u(x+1)^t h(x) \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  
 $h(x)$  is a unit in  $R_n''$  and  $\deg h(x) \leq T_1-t-1 = \begin{cases} 2n-s-1 & \text{if } t < 2s-3n, \\ s-n-t-1 & \text{if } t \geq 2s-3n. \end{cases}$
- **Type 2.3:**  $\langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)) \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  
 $l > s-n-t$ ,  $h_1(x), h_2(x)$  are units in  $R_n''$ ,  $\deg h_1(x) \leq T_1-t-1$  and  $\deg h_2(x) \leq n-t-l-1$ .
- **Type 3.0:**  $\langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $1 \leq s \leq n-1$ ,  $0 \leq t < m < s$ ,  
 $h(x)$  is either zero or a unit in  $R_n''$  and  $\deg h(x) \leq m-t-1$ .
- **Type 3.1:**  $\langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n \leq s \leq 2n-1$ ,  $0 \leq t < n$ ,  $1+t \leq m < T$ ,  
 $h(x)$  is either zero or a unit in  $R_n''$  and  $\deg h(x) \leq m-t-1$ .
- **Type 3.2:**  $\langle (x+1)^s + 2u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  
 $1+t \leq m < n$ ,  $h(x)$  is a unit in  $R_n''$  and  $\deg h(x) \leq \min\{m, T_1\} - t - 1$ .
- **Type 3.3:**  $\langle (x+1)^s + 2u(x+1)^t h(x), 2u(x+1)^{m_1} \rangle$ , where  $n \leq s \leq 2n-1$ ,  
 $0 \leq t < s-n$ ,  $1+t \leq m_1 < T_1$ ,  $h(x)$  is a unit in  $R_n''$  and  $\deg h(x) \leq m_1 - t - 1$ .
- **Type 3.4:**  $\langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  
 $0 \leq t < s-n$ ,  $t+l < m < n$ ,  $h_1(x), h_2(x)$  are units in  $R_n''$ .
- **Type 3.5:**  $\langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), 2u(x+1)^{m_1} \rangle$ , where  $n < s \leq 2n-1$ ,  
 $0 \leq t < s-n$ ,  $1+t < m_1 < T_1$ ,  $h_1(x), h_2(x)$  are units in  $R_n''$ .

In the following Theorems 30 and 32, we give the annihilators of each ideal of types described in Theorem 29.

**Theorem 30.** Let  $I$  be a non-trivial principal ideal and  $A(I)$  be its annihilator in  $R_n$ .

- (a) If  $I = \langle u(x+1)^m \rangle$ , where  $0 \leq m \leq 2n-1$ , then  $A(I) = \langle (x+1)^{2n-m}, u \rangle$ .  
(b) If  $I = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $1 \leq s \leq n-1$ ,  $0 \leq t < s$ ,  $h(x)$  is either zero or a unit in  $R_n''$  and  $\deg h(x) \leq s-t-1$ , then

$$A(I) = \begin{cases} \langle (x+1)^{2n-s} + u(x+1)^{2n-2s+t} h(x) \rangle, & \text{when } t < 2s-n, \\ \langle (x+1)^{2n-s} + 2u(x+1)^{n-2s+t} (1 + (1+x)^{\frac{n}{2}}) h(x) \rangle, & \text{when } t \geq 2s-n. \end{cases}$$

- (c) If  $I = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $n \leq s \leq 2n-1$ ,  $0 \leq t \leq n-1$  and  $h(x)$  is either zero or a unit in  $R_n''$ , then

$$A(I) = \begin{cases} \langle (x+1)^{s-t} + u h(x), u(x+1)^{2n-s} \rangle, & \text{when } t < 2s-2n, \\ \langle (x+1)^{2n-s} + u(x+1)^{2n-2s+t} h(x) \rangle, & \text{when } t \geq 2s-2n. \end{cases}$$

- (d) If  $I = \langle (x+1)^s + 2u(x+1)^t h(x) \rangle$ , where  $n < s \leq 2n-1$  and  $0 \leq t < s-n$  and  $h(x)$  is a unit in  $R_n''$ , then

$$A(I) = \begin{cases} \langle (x+1)^{2n-s} + u(x+1)^{3n-2s+t} (1 + (x+1)^{\frac{n}{2}}) h(x) \rangle, & \text{when } 2s-3n \leq t < s-n, \\ \langle (x+1)^{n-t}, u(x+1)^{2n-s} \rangle, & \text{when } t < 2s-3n. \end{cases}$$

- (e) If  $I = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)) \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$  and  $h_1(x), h_2(x)$  are units in  $R_n''$ , then

$$A(I) = \langle (x+1)^{s-t} + u(2h_1(x) + (x+1)^l h_2(x)), u(x+1)^{2n-s} \rangle.$$

**Corollary 31.** Let  $C$  be a non-trivial principal negacyclic code of length  $n$  over  $R$ . Then the dual  $C^\perp$  of  $C$  is given as follows:

- (a) If  $C = \langle u(x+1)^m \rangle$ , where  $1 \leq m \leq 2n-1$ , then  $C^\perp = \langle (x+1)^{2n-m}, u \rangle$ .  
(b) If  $C = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $1 \leq s \leq n-1$ ,  $0 \leq t < s$  and  $h(x)$  is either zero or a unit in  $R_n''$ , then

$$C^\perp = \begin{cases} \langle (x+1)^{2n-s} + ux^{s-t} (x+1)^{2n-2s+t} h\left(\frac{1}{x}\right) \rangle, & \text{when } t < 2s-n, \\ \langle (x+1)^{2n-s} + 2ux^{n+s-t-\frac{n}{2}} (x+1)^{n-2s+t} h\left(\frac{1}{x}\right) \rangle, & \text{when } t \geq 2s-n. \end{cases}$$

- (c) If  $C = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $n \leq s \leq 2n-1$ ,  $0 \leq t \leq n-1$  and  $h(x)$  is either zero or a unit in  $R_n''$ , then

$$C^\perp = \begin{cases} \langle (x+1)^{s-t} + ux^{s-t} h\left(\frac{1}{x}\right), u(x+1)^{2n-s} \rangle, & \text{when } t < 2s-2n, \\ \langle (x+1)^{2n-s} + ux^{s-t} (x+1)^{2n-2s+t} h\left(\frac{1}{x}\right) \rangle, & \text{when } t \geq 2s-2n. \end{cases}$$

- (d) If  $C = \langle (x+1)^s + 2u(x+1)^t h(x) \rangle$ , where  $n < s \leq 2n-1$  and  $0 \leq t < s-n$  and  $h(x)$  is a unit in  $R_n''$ , then

$$C^\perp = \begin{cases} \langle (x+1)^{2n-s} + ux^{s-n-t} (x+1)^{3n-2s+t} \left(1 + \left(\frac{1}{x} + 1\right)^{\frac{n}{2}}\right) h\left(\frac{1}{x}\right) \rangle, & \text{when } 2s-3n \leq t < s-n, \\ \langle (x+1)^{n-t}, u(x+1)^{2n-s} \rangle, & \text{when } t < 2s-3n. \end{cases}$$

- (e) If  $C = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)) \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$  and  $h_1(x), h_2(x)$  are units in  $R_n''$ , then

$$C^\perp = \left\langle (x+1)^{s-t} + u \left( 2x^{s-t} h_1\left(\frac{1}{x}\right) + x^{s-t-l} (x+1)^l h_2\left(\frac{1}{x}\right) \right), u(x+1)^{2n-s} \right\rangle.$$

**Theorem 32.** Let  $I$  be a non-principal ideal and  $A(I)$  be its annihilator in  $R_n$ .

- (a) If  $I = \langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $1 \leq s < n$ ,  $0 \leq t < m < s$  and  $h(x)$  is either zero or a unit in  $R_n''$ , then

$$A(I) = \langle (x+1)^{2n-m} + u(x+1)^{2n-m-s+t} h(x), u(x+1)^{2n-s} \rangle.$$

- (b) If  $I = \langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n \leq s < 2n$ ,  $0 \leq t < n$ ,  $1+t \leq m < T$  and  $h(x)$  is either zero or a unit in  $R_n''$ , then

$$A(I) = \begin{cases} \langle (x+1)^{2n-m} + u(x+1)^{2n-m-s+t} h(x), u(x+1)^{2n-s} \rangle, & \text{when } t \geq s+m-2n, \\ \langle (x+1)^{s-t} + u h(x), u(x+1)^{2n-s} \rangle, & \text{when } t < s+m-2n. \end{cases}$$

- (c) If  $I = \langle (x+1)^s + 2u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m < n$  and  $h(x)$  is a unit in  $R_n''$ , then

$$A(I) = \langle (x+1)^{2n-m}, u(x+1)^{2n-s} \rangle.$$

- (d) If  $I = \langle (x+1)^s + 2u(x+1)^t h(x), 2u(x+1)^{m_1} \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m_1 < T_1$  and  $h(x)$  is a unit in  $R_n''$ , then

$$A(I) = \begin{cases} \langle (x+1)^{n-m_1} + u(x+1)^{2n-m-s+t} (1 + (x+1)^{\frac{n}{2}}) h(x), u(x+1)^{2n-s} \rangle, & \text{when } t \geq s+m_1-2n, \\ \langle (x+1)^{n-t}, u(x+1)^{2n-s} \rangle, & \text{when } t < s+m_1-2n. \end{cases}$$

- (e) If  $I = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $t+l+1 \leq m < n$  and  $h_1(x), h_2(x)$  are units in  $R_n''$  then

$$A(I) = \begin{cases} \langle (x+1)^{2n-m} + u(x+1)^{2n-m-s+t+l} h_2(x), u(x+1)^{2n-s} \rangle, & \text{when } t+l \geq s+m-2n, \\ \langle (x+1)^{2n-l}, u(x+1)^{2n-s} \rangle, & \text{when } t+l < s+m-2n. \end{cases}$$

- (f) If  $I = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), 2u(x+1)^{m_1} \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $t < m_1 < T_1$  and  $h_1(x), h_2(x)$  are units in  $R_n''$ , then

$$A(I) = \begin{cases} \langle (x+1)^{n-m_1} + u(x+1)^{n-m_1-s+t+l} h'(x), u(x+1)^{2n-s} \rangle, & \text{when } t+l \geq s+m_1-n, \\ \langle (x+1)^{2n-l}, u(x+1)^{2n-s} \rangle, & \text{when } t+l < s+m_1-n, \end{cases}$$

$$\text{where } h'(x) = (h_1(x)(x+1)^{n-l} + h_2(x)(1 + (x+1)^{\frac{n}{2}})).$$

**Corollary 33.** Let  $C$  be a non-principal negacyclic code of length  $n$  over  $R$ . Then the dual  $C^\perp$  of  $C$  is given as follows:

- (a) If  $C = \langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $1 \leq s < n$  and  $0 \leq t < m < s$  and  $h(x)$  is either zero or a unit in  $R_n''$ , then

$$C^\perp = \left\langle (x+1)^{2n-m} + ux^{s-t}(x+1)^{2n-m-s+t} h\left(\frac{1}{x}\right), u(x+1)^{2n-s} \right\rangle.$$

- (b) If  $C = \langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n \leq s < 2n$  and  $0 \leq t < n$ ,  $1+t \leq m < T$  and  $h(x)$  is either zero or a unit in  $R_n''$ , then

$$C^\perp = \begin{cases} \langle (x+1)^{2n-m} + ux^{s-t}(x+1)^{2n-m-s+t} h\left(\frac{1}{x}\right), u(x+1)^{2n-s} \rangle, & \text{when } t \geq s+m-2n, \\ \langle (x+1)^{s-t} + ux^{s-t} h\left(\frac{1}{x}\right), u(x+1)^{2n-s} \rangle, & \text{when } t < s+m-2n. \end{cases}$$

(c) If  $C = \langle (x+1)^s + 2u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m < n$  and  $h(x)$  is a unit in  $R_n''$ , then

$$C^\perp = \langle (x+1)^{2n-m}, u(x+1)^{2n-s} \rangle.$$

(d) If  $C = \langle (x+1)^s + 2u(x+1)^t h(x), 2u(x+1)^{m_1} \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m_1 < T_1$  and  $h(x)$  is a unit in  $R_n''$ , then

$$C^\perp = \begin{cases} \langle (x+1)^{n-m_1} + ux^{s-n-t}(x+1)^{2n-m_1-s+t} h'(x), u(x+1)^{2n-s} \rangle, & \text{when } t \geq s+m_1-2n, \\ \langle (x+1)^{n-t}, u(x+1)^{2n-s} \rangle, & \text{when } t < s+m_1-2n, \end{cases}$$

where  $h'(x) = (1 + (\frac{1}{x} + 1)^{\frac{n}{2}})h(\frac{1}{x})$ .

(e) If  $C = \langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$ ,  $t+l+1 \leq m < n$  and  $h_1(x), h_2(x)$  are units in  $R_n''$ , then

$$C^\perp = \begin{cases} \langle (x+1)^{2n-m} + ux^{s-t-l}(x+1)^{2n-m-s+t+l} h_2(\frac{1}{x}), u(x+1)^{2n-s} \rangle, & \text{when } t+l \geq s+m-2n, \\ \langle (x+1)^{2n-l}, u(x+1)^{2n-s} \rangle, & \text{when } t+l < s+m-2n. \end{cases}$$

(f) If  $C = \langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)), 2u(x+1)^{m_1} \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$ ,  $t < m_1 < T_1$  and  $h_1(x), h_2(x)$  are units in  $R_n''$ , then

$$C^\perp = \begin{cases} \langle (x+1)^{n-m_1} + ux^{s-t-l}(x+1)^{n-m_1-s+t+l} h''(x), u(x+1)^{2n-s} \rangle, & \text{when } t+l \geq s+m_1-n, \\ \langle (x+1)^{2n-l}, u(x+1)^{2n-s} \rangle, & \text{when } t+l < s+m_1-n, \end{cases}$$

where  $h''(x) = h_1(\frac{1}{x})(\frac{1}{x} + 1)^{n-l} + h_2(\frac{1}{x})(1 + (\frac{1}{x} + 1)^{\frac{n}{2}})$ .

Now we consider the cardinality of the negacyclic code  $C$  over  $R$ . If  $|\text{Tor}(C)|$  and  $|\text{Res}(C)|$  are known, then  $|C|$  can be computed by  $|C| = |\text{Tor}(C)||\text{Res}(C)|$ . The following theorem gives the  $\text{Tor}(C)$  and  $\text{Res}(C)$  of  $C$  in each case.

**Lemma 34.** [12, Theorem 6.10] The negacyclic codes of length  $n$  over  $\mathbb{Z}_4$  are precisely the ideals  $\langle (x+1)^i \rangle$ ,  $0 \leq i \leq 2n$ , of  $\frac{\mathbb{Z}_4[x]}{(x^n+1)}$ .

**Lemma 35.** [12, Theorem 6.14] Let  $\mathcal{C} = \langle (x+1)^i \rangle$ ,  $0 \leq i \leq 2n$  be a negacyclic code of length  $n$  over  $\mathbb{Z}_4$ . Then  $|\mathcal{C}| = 2^{2n-i}$ .

**Theorem 36.** Let  $C$  be a non-trivial negacyclic code of length  $n$  over  $R$ .

- (a) If  $C = \langle u(x+1)^m \rangle$ , where  $0 \leq m \leq 2n$ , then  $\text{Res}(C) = \langle 0 \rangle$  and  $\text{Tor}(C) = \langle (x+1)^m \rangle$ .
- (b) If  $C = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $0 \leq s \leq n-1$ ,  $0 \leq t < s$  and  $h(x)$  either zero or a unit in  $R_n''$ , then  $\text{Res}(C) = \text{Tor}(C) = \langle (x+1)^s \rangle$ .
- (c) If  $C = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $n \leq s \leq 2n-1$ ,  $0 \leq t < n$  and  $h(x)$  either zero or a unit in  $R_n''$ , then  $\text{Res}(C) = \langle (x+1)^s \rangle$  and  $\text{Tor}(C) = \langle (x+1)^T \rangle$ .
- (d) If  $C = \langle (x+1)^s + 2u(x+1)^t h(x) \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $h(x)$  is a unit in  $R_n''$ , then  $\text{Res}(C) = \langle (x+1)^s \rangle$  and  $\text{Tor}(C) = \langle (x+1)^T \rangle$ .
- (e) If  $C = \langle (x+1)^s + u(x+1)^t(2h_1(x) + (x+1)^l h_2(x)) \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$ ,  $h_1(x)$  and  $h_2(x)$  are units in  $R_n''$ , then  $\text{Res}(C) = \langle (x+1)^s \rangle$  and  $\text{Tor}(C) = \langle (x+1)^T \rangle$ , where  $T = \min\{s, 2n-s+t+l\}$ .

- (f) If  $C = \langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $1 \leq s \leq n-1$ ,  $0 \leq t < m < s$ ,  $h(x)$  is either zero or a unit in  $R_n''$ , then  $\text{Res}(C) = \langle (x+1)^s \rangle$  and  $\text{Tor}(C) = \langle (x+1)^m \rangle$ .
- (g) If  $C = \langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n \leq s \leq 2n-1$ ,  $0 \leq t < n$ ,  $1+t \leq m < T$ ,  $h(x)$  is either zero or a unit in  $R_n''$ , then  $\text{Res}(C) = \langle (x+1)^s \rangle$  and  $\text{Tor}(C) = \langle (x+1)^m \rangle$ .
- (h) If  $C = \langle (x+1)^s + 2u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m < n$ ,  $h(x)$  is a unit in  $R_n''$ , then  $\text{Res}(C) = \langle (x+1)^s \rangle$  and  $\text{Tor}(C) = \langle (x+1)^m \rangle$ .
- (i) If  $C = \langle (x+1)^s + 2u(x+1)^t h(x), 2u(x+1)^{m_1} \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m_1 < T_1$ ,  $h(x)$  is a unit in  $R_n''$ , then  $\text{Res}(C) = \langle (x+1)^s \rangle$  and  $\text{Tor}(C) = \langle (x+1)^{n+m_1} \rangle$ .
- (j) If  $C = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$ ,  $l+t < m < n$  and  $h_1(x), h_2(x)$  are units in  $R_n''$ , then  $\text{Res}(C) = \langle (x+1)^s \rangle$  and  $\text{Tor}(C) = \langle (x+1)^m \rangle$ .
- (k) If  $C = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), 2u(x+1)^{m_1} \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$ ,  $t < m_1 < T_1$  and  $h_1(x), h_2(x)$  are units in  $R_n''$ , then  $\text{Res}(C) = \langle (x+1)^s \rangle$  and  $\text{Tor}(C) = \langle (x+1)^{n+m_1} \rangle$ .

**Theorem 37.** Let  $C$  be a negacyclic code of length  $n$  over  $R$ . Then

- (a) If  $C = \langle u(x+1)^m \rangle$ , where  $0 \leq m \leq 2n$ , then  $|C| = 2^{2n-m}$ .
- (b) If  $C = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $0 \leq s \leq n-1$ ,  $0 \leq t < s$ , then  $|C| = 4^{2n-s}$ .
- (c) If  $C = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $n \leq s \leq 2n-1$ ,  $0 \leq t < n$ , then

$$|C| = \begin{cases} 2^{2n-t} & \text{if } 0 \leq t < 2s-2n, \\ 4^{2n-s} & \text{if } t \geq 2s-2n. \end{cases}$$

- (d) If  $C = \langle (x+1)^s + 2u(x+1)^t h(x) \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ , then

$$|C| = \begin{cases} 2^{n-t} & \text{if } 0 \leq t < 2s-3n, \\ 4^{2n-s} & \text{if } 2s-3n \leq t < s-n. \end{cases}$$

- (e) If  $C = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)) \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$  and  $l > s-n-t$ , then

$$|C| = \begin{cases} 2^{2n-l-t} & \text{if } s-n < l+t < 2s-2n, \\ 4^{2n-s} & \text{if } l+t \geq 2s-2n. \end{cases}$$

- (f) If  $C = \langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $1 \leq s \leq n-1$ ,  $0 \leq t < m < s$ ,  $h(x)$  is either zero or a unit in  $R_n''$ , then  $|C| = 2^{4n-(m+s)}$ .
- (g) If  $C = \langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n \leq s \leq 2n-1$ ,  $0 \leq t < n$ ,  $1+t \leq m < T$ ,  $h(x)$  is either zero or a unit in  $R_n''$ , then  $|C| = 2^{4n-(m+s)}$ .
- (h) If  $C = \langle (x+1)^s + 2u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m < n$ ,  $h(x)$  is a unit in  $R_n''$ , then  $|C| = 2^{4n-(m+s)}$ .
- (i) If  $C = \langle (x+1)^s + 2u(x+1)^t h(x), 2u(x+1)^{m_1} \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m_1 < T_1$ ,  $h(x)$  is a unit in  $R_n''$ , then  $|C| = 2^{3n-(m_1+s)}$ .
- (j) If  $C = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$ ,  $l+t < m < n$  and  $h_1(x), h_2(x)$  are units in  $R_n''$ , then  $|C| = 2^{4n-(m+s)}$ .
- (k) If  $C = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), 2u(x+1)^{m_1} \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$ ,  $t < m_1 < T_1$  and  $h_1(x), h_2(x)$  are units in  $R_n''$ , then  $|C| = 2^{3n-(m_1+s)}$ .

The following Theorem gives the self-orthogonal negacyclic codes over  $R$ .

**Theorem 38.** *The self-orthogonal negacyclic codes of length  $n$  over  $R$  are:*

- (a)  $C = \langle u(x+1)^m \rangle$ , where  $0 \leq m \leq 2n$ .
- (b)  $C = \langle (x+1)^s + u(x+1)^t h(x) \rangle$ , where  $n \leq s \leq 2n-1$ ,  $0 \leq t < n$  and  $h(x)$  is either zero or a unit in  $R_n''$ .
- (c)  $C = \langle (x+1)^s + 2u(x+1)^t h(x) \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$  and  $h(x)$  is a unit in  $R_n''$ .
- (d)  $C = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)) \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$  and  $h_1(x), h_2(x)$  are units in  $R_n''$ .
- (e)  $C = \langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n \leq s \leq 2n-1$ ,  $0 \leq t < m < T$ ,  $h(x)$  is either zero or a unit in  $R_n''$ , and  $s+m \geq 2n$ .
- (f)  $C = \langle (x+1)^s + 2u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m < n$ ,  $h(x)$  is a unit in  $R_n''$ , and  $s+m \geq 2n$ .
- (g)  $C = \langle (x+1)^s + 2u(x+1)^t h(x), 2u(x+1)^{m_1} \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m_1 < T_1$ ,  $h(x)$  is a unit in  $R_n''$ , and  $s+m_1 \geq n$ .
- (h)  $C = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$ ,  $t+l < m < n$ ,  $h_1(x), h_2(x)$  are units in  $R_n''$ , and  $s+m \geq 2n$ .
- (i)  $C = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), 2u(x+1)^{m_1} \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$ ,  $t < m_1 < T_1$ ,  $h_1(x), h_2(x)$  are units in  $R_n''$ , and  $s+m_1 \geq n$ .

In the following theorem we list all self-dual negacyclic codes of length  $n$  over  $R$ .

**Theorem 39.** *The only self-dual negacyclic codes of length  $n$  over  $R$  are:*

- (a)  $C = \langle (x+1)^n + u(x+1)^t h(x) \rangle$ , where  $t \geq 0$  and  $h(x)$  is either zero or a unit in  $R_n''$ .
- (b)  $C = \langle (x+1)^s + uh(x) \rangle$ , where  $n < s \leq 2n-1$ ,  $h(x)$  is either zero or a unit in  $R_n''$ .
- (c)  $C = \langle (x+1)^s + u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n \leq s \leq 2n-1$ ,  $0 \leq t < m < T$ ,  $h(x)$  is either zero or a unit in  $R_n''$  and  $s+m = 2n$ .
- (d)  $C = \langle (x+1)^s + 2u(x+1)^t h(x), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m < n$ ,  $h(x)$  is a unit in  $R_n''$  and  $s+m = 2n$ .
- (e)  $C = \langle (x+1)^s + 2u(x+1)^t h(x), 2u(x+1)^{m_1} \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $1+t \leq m_1 < T_1$ ,  $h(x)$  is a unit in  $R_n''$  and  $s+m_1 = n$ .
- (f)  $C = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), u(x+1)^m \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$ ,  $t+l < m < n$ ,  $h_1(x), h_2(x)$  are units in  $R_n''$ , and  $s+m = 2n$ .
- (g)  $C = \langle (x+1)^s + u(x+1)^t (2h_1(x) + (x+1)^l h_2(x)), 2u(x+1)^{m_1} \rangle$ , where  $n < s \leq 2n-1$ ,  $0 \leq t < s-n$ ,  $l > s-n-t$ ,  $t < m_1 < T_1$ ,  $h_1(x), h_2(x)$  are units in  $R_n''$ , and  $s+m_1 = n$ .

**Example 6.** For  $n = 2$ ,  $R_2 = \frac{R[x]}{\langle x^2+1 \rangle}$  has 24 ideals (negacyclic codes of length 2 over  $R$ ), out of which 7 are self-dual ( $C^*$ ) and 8 are self-orthogonal ( $C^\dagger$ ). They are listed below:

Negacyclic code $C$	Annihilator $A(C)$	Size of $C$
$C_1 = \langle 0 \rangle$	$C_2$	1
$C_2 = \langle 1 \rangle$	$C_1$	256
$C_3 = \langle u \rangle$	$C_3^*$	16
$C_4 = \langle u(x+1) \rangle$	$C_{22}^\dagger$	8
$C_5 = \langle u(x+1)^2 \rangle$	$C_{19}^\dagger$	4
$C_6 = \langle u(x+1)^3 \rangle$	$C_{18}^\dagger$	2
$C_7 = \langle (x+1) \rangle$	$C_9$	64
$C_8 = \langle (x+1)^2 \rangle$	$C_8^*$	16
$C_9 = \langle (x+1)^3 \rangle$	$C_7^\dagger$	4
$C_{10} = \langle (x+1) + u \rangle$	$C_{16}$	64
$C_{11} = \langle (x+1)^2 + u \rangle$	$C_{11}^*$	16
$C_{12} = \langle (x+1)^2 + u(x+1) \rangle$	$C_{12}^*$	16
$C_{13} = \langle (x+1)^2 + u(1 + (x+1)) \rangle$	$C_{13}^*$	16
$C_{14} = \langle (x+1)^3 + u \rangle$	$C_{14}^*$	16
$C_{15} = \langle (x+1)^3 + u(x+1) \rangle$	$C_{21}^\dagger$	8
$C_{16} = \langle (x+1)^3 + 2u \rangle$	$C_{10}^\dagger$	4
$C_{17} = \langle (x+1), u \rangle$	$C_6$	128
$C_{18} = \langle (x+1)^2, u \rangle$	$C_5$	64
$C_{19} = \langle (x+1)^2, u(x+1) \rangle$	$C_{24}$	32
$C_{20} = \langle (x+1)^2 + u, u(x+1) \rangle$	$C_{15}$	32
$C_{21} = \langle (x+1)^3, u \rangle$	$C_4$	32
$C_{22} = \langle (x+1)^3, u(x+1) \rangle$	$C_{23}^*$	16
$C_{23} = \langle (x+1)^3, 2u \rangle$	$C_{20}^\dagger$	8
$C_{24} = \langle (x+1)^3 + 2u, u(x+1) \rangle$	$C_{23}^\dagger$	16

## 5. Conclusion

In this paper we have studied some structural properties of negacyclic codes over the ring  $R = \mathbb{Z}_4 + u\mathbb{Z}_4$  for both odd length and length  $2^k$ . Since  $R$  is not a principal ideal ring, the ideal structure of  $\frac{R[x]}{\langle x^n+1 \rangle}$  is not as well understood. We have studied some properties of principally generated negacyclic codes of odd length over  $R$ . We have obtained the structure of ideals of  $\frac{R[x]}{\langle x^{2^k}+1 \rangle}$ . We have also studied self-orthogonal and self-dual negacyclic codes length  $2^k$  over  $R$ .

## References

- [1] Abualrub, T. and Oehmke, R., "Cyclic codes of length  $2^e$  over  $\mathbb{Z}_4$ ", *Discrete Applied Mathematics*, Vol. 128, pp. 3–9, 2003.
- [2] Abualrub, T. and Oehmke, R., "On the generators of  $\mathbb{Z}_4$  cyclic codes of length  $2^e$ ", *IEEE Trans. Inf. Theory*, Vol. 49, No. 9, pp. 2126–2133, 2003.



- [3] Bandi, R. K. and Bhaintwal, M., “Cyclic codes over  $\mathbb{Z}_4 + u\mathbb{Z}_4$ ”, *submitted to Adv. Math. Commun., s. Am. Inst. Math. Sci. (AIMS)*.
- [4] Berlekamp, E. R., “Negacyclic codes for the Lee metric, in *Proc. Conf. Combinatorial Mathematics and Its Applications*. Chapel Hill, N.C.: Univ. North Carolina Press, pp. 298–316, 1968.
- [5] Blackford, T., “Negacyclic codes over  $\mathbb{Z}_4$  of even length”, *IEEE Trans. Inf. Theory*, Vol. 49, No. 6, pp. 1417–1424, 2003.
- [6] Blackford, T., “Cyclic codes over of oddly even length, *Appl. Discr. Math.*, vol. 128, pp. 27–46, 2003.
- [7] Bonnecaze, P. and Udaya, P., “Negacyclic codes and self-dual codes over the ring  $\mathbb{F}_2 + u\mathbb{F}_2$ ”, *IEEE Trans. Inf. Theory*, Vol. 45, No. 4, pp. 1250–1255, 1999.
- [8] Castagnoli, G., Massey, J. L., Schoeller, P. A., and Seemann, N. V., “On repeated-root cyclic codes, *IEEE Trans. Inf. Theory*, vol. 37, pp. 337–342, 1991.
- [9] Dinh, H. Q., “Complete distances of all negacyclic codes of length  $2^s$  over  $\mathbb{Z}_{2^a}$ ”, *IEEE Trans. Inf. Theory*, Vol. 53, No. 1, pp. 147–161, 2007.
- [10] Dinh, H. Q., “Constacyclic codes of length  $2^s$  over Galois extension of rings  $\mathbb{F}_2 + u\mathbb{F}_2$ ”, *IEEE Trans. Inf. Theory*, Vol. 55, No. 4, pp. 1730–1740, 2009.
- [11] Dinh, H. Q., “Constacyclic codes of length  $p^s$  over  $\mathbb{F}_{p^m} + u\mathbb{F}_{p^m}$ ”, *Journal of Algebra*, Vol. 324, pp. 940–950, 2010.
- [12] Dinh, H. Q., “Negacyclic codes of length  $2^s$  over Galois rings”, *IEEE Trans. Inf. Theory*, Vol. 51, No. 12, pp. 4252–4262, 2005.
- [13] Dinh, H. Q. and Permouth, S. R. L., “Cyclic codes and negacyclic codes over finite chain ring”, *IEEE Trans. Inf. Theory*, Vol. 50, No. 8, pp. 1728–1744, 2004.
- [14] Dougherty, S. T. and Ling, S., “Cyclic codes over  $\mathbb{Z}_4$  of even length”, *Des. Codes Cryptogr.*, 39, pp. 127–153, 2006.
- [15] Hammons, A., Kumar, P. V., Calderbank A. R., Slone N. J. A. and Solé P., “The  $\mathbb{Z}_4$  linearity of Kerdock, Preparata, Goethals and related codes”, *IEEE Trans. Inf. Theory*, Vol. 40, No. 4, pp. 301–319, 1994.
- [16] Lint, J. H. V., “Repeated-root cyclic codes, *IEEE Trans. Inf. Theory*, vol. 37, pp. 343–345, 1991.
- [17] MacWilliams, F. J. and Sloane, N. J. A., *The Theory of Error Correcting Codes*, North Holland, 1977.
- [18] McDonald, B. R., *Finite Rings with Identity*, Marcel Dekker, 1974.
- [19] Norton, G. and Salagean, A., “On the structure of linear and cyclic codes over a finite chain ring”, *Appl. Algebra Engrg. Comm. Comput.*, Vol. 10, No. 6, pp. 489–506, 2000.
- [20] Pless, V. S. and Qian, Z., “Cyclic codes and quadratic residue codes over  $\mathbb{Z}_4$ ”, *IEEE Trans. Inf. Theory*, Vol. 42, No. 5, pp. 1594–1600, 1996.
- [21] Tang, L. Z., Soh, C. B. and Gunawan, E., “A note on the q-ary image of a q-ary repeated-root cyclic code, *IEEE Trans. Inf. Theory*, vol. 43, pp. 732–737, 1997.

- [22] Wolfmann J., “Negacyclic and cyclic codes over  $\mathbb{Z}_4$ ”, *IEEE Trans. Inf. Theory*, Vol. 45, No. 7, pp. 2527–2532, 1999.
- [23] Yildiz, B. and Karadeniz, S., “Cyclic codes over  $\mathbb{F}_2 + u\mathbb{F}_2 + v\mathbb{F}_2 + uv\mathbb{F}_2$ ”, *Des. Codes Cryptogr.*, Vol. 58, No. 3, pp. 221–234, 2011.
- [24] Yildiz, B. and Karadeniz, S., “Linear codes over  $\mathbb{Z}_4 + u\mathbb{Z}_4$ , MacWilliams identities, projections, and formally self-dual codes”, *Finite Fields Appl.* 27, pp. 24–40, 2014.
- [25] Zhu, S., Wang, Y. and Shi, M. “Some results on negacyclic codes over  $\mathbb{F}_2 + v\mathbb{F}_2$ ”, *IEEE Trans. Inf. Theory*, Vol. 56, No. 4, pp. 1680–1684, 2010.
- [26] Zimmermann, K. H., “On generalizations of repeated-root cyclic codes”, *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 641–649, 1996.